IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

BABY DOE, *et al.*, Plaintiffs, -v.- JOSHUA MAST, *et al.*, Defendants,	CIVIL NO: 3:22-cv-00049-NKM-JCH

DEFENDANT JOSHUA MAST'S OBJECTIONS AND
STATEMENT REGARDING PLAINTIFFS' SECOND REQUESTS FOR ADMISSIONS

Defendant Joshua Mast, pursuant to Fed. R. Civ. P. 36, submits the following objections and statement regarding the second requests for admissions ("Requests") propounded by Plaintiffs John Doe and Jane Doe (collectively, "Plaintiffs").

OBJECTIONS TO INSTRUCTIONS AND REQUESTS

Joshua Mast objects to Plaintiffs' excessive number of requests for admission that Plaintiffs are using to circumvent their limits on interrogatories, requests for production, and depositions. Plaintiffs previously issued 47 requests for admission in April 2023 and now have issued 80 additional requests, all related to topics that are more appropriately sought by the normal means of discovery—interrogatories, requests for production, and depositions. *See, e.g.*, *California v. The Jules Fribourg*, 19 F.R.D. 432, 434 (N.D. Cal. 1955) ("[I]nterrogatories and requests for admissions are not interchangeable procedures designed for the same purpose."); *In re Olympia Holding Corp.*, 189 B.R. 846, 853 (Bankr. M.D. Fla. 1995) ("Utilizing interrogatories disguised as requests for admissions in an attempt to circumvent a . . . rule limiting the number of interrogatories is an abuse of the discovery process." (citing *Misco, Inc. v. U.S. Steel Corp.*, 784 F.2d 198, 206 (6th Cir. 1986))).

Plaintiffs cannot use requests for admission to circumvent the numerical limited in Federal Rule of Civil Procedure 33(a). *Safeco of Am. v. Rawstron*, 181 F.R.D. 441, 445 (C.D. Cal. 1998).

Joshua Mast further objects because the definition "Litigation Relating to Baby Doe" is vague, overbroad, and imprecise. As relayed in the definition, there are at least five different matters involving the Child at issue in this case—all of which were at different times spanning a period of almost five years, and which involve different parties and different orders from different courts concerning what Joshua Mast could say publicly and regarding what documents Joshua Mast could hold in his possession. It is not reasonable for Joshua Mast to provide responses with certitude to these compound requests that seek information relating to at least five different complex cases.

Further, Joshua Mast objects to the definition of "Litigation Relating to Baby Doe" because that definition insinuates that the Protective Order in this case—which should be revoked (*see* ECF No. 130)—was always in effect when it was not entered until September 2022. As such, the Requests relate to information entirely irrelevant to any issue related to any aspect of the case and especially to the claims in Plaintiffs' Complaint, which relate only to events that occurred between September 2019—when the Child was recovered from a battlefield after her parents fought U.S. forces to the death—and September 2021—when Joshua Mast lawfully took possession of his adopted daughter, the Child at issue in this litigation.

STATEMENT REGARDING REQUESTS

Consistent with these objections, Joshua Mast cannot respond to the voluminous and vague Requests for Admission, but he will provide this short statement in an effort to provide clarification for the benefit of Plaintiffs. As Joshua Mast has relayed to Plaintiffs' counsel on several occasions, he has fully complied with all discovery obligations throughout both the federal and state court litigation. Recently, he has provided the Does with entire responses to their extensive and burdensome Requests for Production, subject to non-party United States' review of all materials that

must be approved pursuant to *United States ex rel. Touhy v. Ragen*, 340 U.S. 462 (1951). Indeed, many of the Requests—*e.g.*, the information requested in Request Nos. 3 and 5—have already been provided to Plaintiffs, and there is no apparent litigation purpose served by demanding granular admissions or denials about basic matters of document production contents. If there are particular emails, for instance, that Plaintiffs seek to authenticate, Joshua Mast will readily confer in good faith about authentication in the normal course.

Joshua Mast has made diligent efforts to comply with all court orders while simultaneously serving in the U.S. military and as a liaison for the many individuals he helped escape Afghanistan after the former Afghan government collapsed in August 2021. In his role as a member of the U.S. military, Joshua Mast has been instructed to use certain settings on his phone for some text message applications, including Signal and WhatsApp, to protect military information and endangered Afghan contacts who still needed to escape Afghanistan. *See* Ex. 1 at 3. Joshua Mast also obtained a new iPhone in December 2021 and believes both Signal and WhatsApp were likely set to their default settings, which kept messages only for a few weeks. Additionally, the time in which messages could be kept in both applications could be changed at any time by other users with whom Joshua Mast messaged and he thus could not control the manner in which all messages were sent or how long the messages were kept. Consistent with how these applications operate, Joshua Mast is not in position to know, let alone certify for a broad period of time, how every message may have been treated under the dynamic message retention settings within these applications.

Simultaneously, during the litigation in Fluvanna County Circuit Court, the parties agreed that Plaintiffs' claims related only to documents prior to December 8, 2021. And during that litigation, the Fluvanna County Circuit Court ordered the parties to destroy certain documents from that litigation. *See generally* Ex. 2; Ex. 3. Those orders included deleting communications containing any of those documents. *See generally id.*

As such, some documents—as apparently defined by Plaintiff John and Jane Doe's broad terms—may not be available at this time either because (1) Joshua Mast was required to do so by the Fluvanna County Circuit Court; (2) he was under no obligation to preserve the documents because they did not, and do not, relate to any of John or Jane Doe's claims—claims that relate only to Joshua Mast's adoption of his daughter, the Child at issue in this litigation; (3) third parties may have used message retention settings that prevented Jousha Mast from retaining messages in the normal course; (4) inadvertent conduct consistent with the normal and reasonable use of messaging applications; and/or (5) technical limitations inherent to the messaging applications or change in cell phone hardware that prevent current access to messages sent years ago.

Many of the other Requests relate to communications that Plaintiffs know Joshua Mast has claimed privilege over and which will be the subject of a motion to quash a subpoena sent to Liberty University (after already previously seeking the same information). In general, Plaintiffs have the Masts' privilege log and can learn the information requested in the Requests simply by examining the log and examining the documents the Masts produced to Plaintiffs.

Other Requests have already been asked and answered or seek basic information about documents that have already been provided to Plaintiffs in discovery, and Joshua Mast thus need not respond to those Requests in granular and improper requests for admission.

Joshua Mast is willing to meet and confer regarding the above.

Dated: February 20, 2024

Respectfully submitted,

/s/ Michael L. Francisco .

John S. Moran (VSB No. 84326)
Michael L. Francisco (*pro hac vice*)
MCGUIREWOODS LLP
888 16th St. N.W., Suite 500
Black Lives Matter Plaza
Washington, DC 20006
T: (202) 828-2817

F: (202) 828-3327
jmoran@mcguirewoods.com
mfrancisco@mcguirewoods.com

CERTIFICATE OF SERVICE

I certify that, on February 20, 2024, I electronically mailed the foregoing to all counsel of record in this case.

Respectfully submitted,

/s/ Michael L. Francisco .
John S. Moran (VSB No. 84326)
Michael L. Francisco (*pro hac vice*)
MCGUIREWOODS LLP
888 16th St. N.W., Suite 500
Black Lives Matter Plaza
Washington, DC 20006
T: (202) 828-2817
F: (202) 828-3327
jmoran@mcguirewoods.com
mfrancisco@mcguirewoods.com

EXHIBIT 1

IDENTITY AWARENESS, PROTECTION, AND MANAGEMENT GUIDE

A GUIDE FOR ONLINE PRIVACY AND SECURITY COMPRISED OF THE COMPLETE COLLECTION OF DEPARTMENT OF DEFENSE SMART CARDS

TWELFTH EDITION, MARCH 2021

BROUGHT TO YOU BY:

U.S. DEPARTMENT OF DEFENSE

HOW TO USE THIS GUIDE

The Identity Awareness, Protection, and Management (IAPM) Guide is a comprehensive resource to help you protect your privacy and secure your identity data online.

The IAPM Guide is divided into chapters detailing key privacy considerations on popular online services, mobile apps, and consumer devices available in the market today. Each section provides you with tools, recommendations, and step-by-step guides to implement settings that maximize your security. The guide is updated periodically.

While some of the chapters in the IAPM Guide deal with technical issues, they do not require a technical background to follow.

The U.S. Department of Defense creates this guide to provide recommendations for readers to keep their identities private and secure online. Please note the information presented here is subject to change.

HIGHLIGHTS FROM THE TWELFTH EDITION!

- A newly consolidated Online Dating chapter
- A newly revamped Video Communications chapter
- Contents updated with the latest mobile operating systems:
    - iOS (v. 14.3) and Android (v. 11)
- Updated chapters, including:
    - Facebook
    - Instagram
    - LinkedIn
    - TikTok
    - Twitter
    - Google Account
    - Messaging Apps
    - Photo Sharing & Storage
    - EXIF Data Removal
    - Video Communications
    - Smartphones
    - Traveling with Smartphones
    - Identity Theft Prevention
    - Securing Home Wi-Fi Network

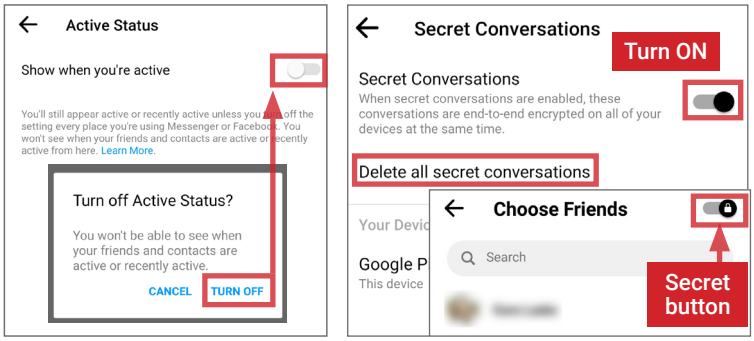
USEFUL LINKS AND RESOURCES

A Parent's Guide to Internet Safety	https://www.fbi.gov/resources/parents
The Balance: Identity Theft 101	https://www.thebalance.com/identity-theft-basics-4073614
Privacy Rights Clearinghouse	http://www.privacyrights.org/privacy-basics
HTTPS Everywhere	https://www.eff.org/https-everywhere
Securing Your Web Browser	https://www.us-cert.gov/publications/securing-your-web-browser

DISCLAIMER:

FACEBOOK MESSENGER

Facebook Messenger allows users to exchange messages, photos, videos, stickers, audio content, stories, files, voice and video calls, and set up group meeting rooms with other Facebook and Instagram users. Messenger offers optional end-to-end encryption for message and voice message conversations supported by Open Whisper System's Signal Protocol.

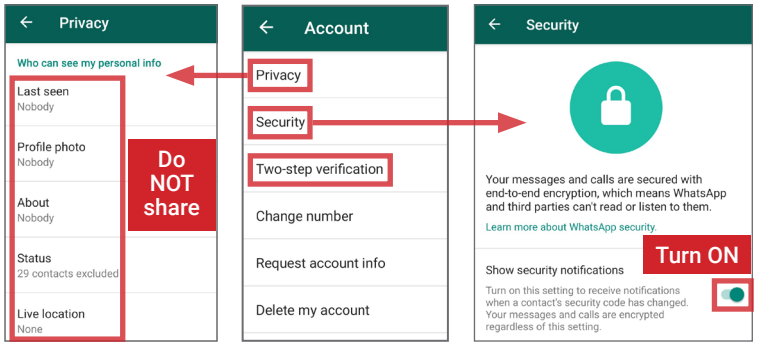


Tap your profile photo to access settings. Under **Profile > Active Status**, **turn OFF Show when you're active.** When starting a new chat, **toggle ON** the **Secret** button [lock icon, upper right] before selecting the recipient. To use the expiring message feature, tap the clock icon in the text box and set the timer.

- Consider using a secondary phone number to create a Messenger account that is not linked to your Facebook or Instagram account.
- Do not link Messenger with your SMS conversations or device contacts
- Always use **Secret Conversations**, and periodically delete conversations.
- If using the **Create Room** feature for group meets, tap the pencil icon [upper right] and set **Who Can Join Automatically** to **People you invite**.

WHATSAPP

WhatsApp provides end-to-end encryption for messages and voice and video calls using Open Whisper System's Signal Protocol. Group messaging can include up to 256 participants, while voice/video calls support up to 4 users. The Broadcast List option enables a user to send the same direct message to up to 256 recipients, rather than using Group Chat. WhatsApp is owned by Facebook, and announced plans to begin sharing user data (including phone number, profile data, and status messages, among others) with Facebook for targeted advertising purposes by February 2021.[19]



Visit **Settings > Chat > Chat backups** to disable video and chat backups.

To maximize security, go to **Settings > Account** and apply the following options:

- Under **Privacy,** set **Who can see my personal info** options to **Nobody.** Do not share your **Status** or **Live location** information.
- Under **Security**, enable **Show security notifications** to view changes in contacts' security codes.
- Enable **Two-step verification** to prevent outside access.
- Periodically delete all conversations.

SIGNAL

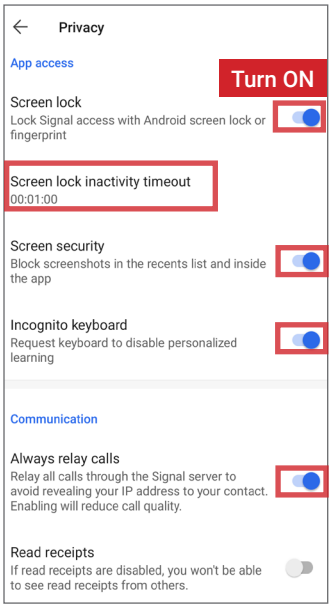
Signal supports end-to-end encrypted communication using Open Whisper System's Signal Protocol. iPhone users can only use Signal to communicate with other Signal users; Android users can contact anyone through the app, but messages with non-Signal users are unencrypted.

In 2018, Signal rolled out a unique **Sealed Sender** feature that also encrypts message sender/recipient information.[18] The app does not collect user metadata or automatically store messages when you backup your device.

Tap the "**...**" icon [upper right] to select **Settings > Privacy** and apply the following options:

- Enable **Screen Lock** and set the inactivity timeout to a short interval.
- Enable the **Screen Security** and **Incognito keyboard** features to limit opportunities for information collection.
- Under **Communication**, toggle on **Always relay calls** to ensure communications do not reveal your IP address.
- Under **Sealed Sender**, enable **Display indicators**
- Under **Signal PIN**, enable **Registration Lock.**

Visit **Settings > Storage > Clear message history** after each completed communication, or set **Keep messages** to 30 days. Never turn on chat backups.



GROUPME

GroupMe is a New York-based mobile messaging app launched in 2010 that was acquired by Microsoft in 2011.[20] GroupMe has 10.75 million active monthly users as of September 2019.[21] Users can register for an account by linking their existing Facebook, Apple, or Microsoft accounts, or with a phone number or email address. Participants in groups can receive and send messages over SMS without registering for a GroupMe account.

GroupMe has a simple settings interface with minimal security and privacy controls.

Navigate to **Settings** and toggle off **Send read receipts for DMs**. Next, tap your profile picture and:

- Enable **Use two-step verification**
- Turn off **Enable sharing**
- Never link your GroupMe to Facebook or Twitter

Note that GroupMe does not use encryption. As a result, user data collected through GroupMe is transmitted unencrypted and can be visible to unintended recipients. This means that the content of communications, as well as the membership and names of groups, can be disclosed to unintended parties.

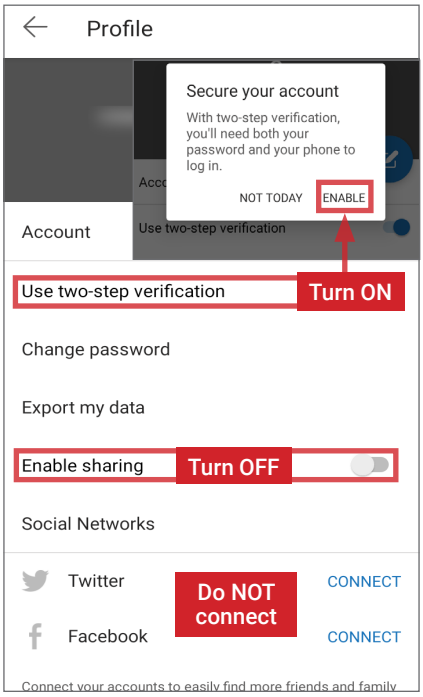


EXHIBIT 2

CLERK'S OFFICE

FLUVANNA COUNTY CIRCUIT COURT

POST OFFICE BOX 550

PALMYRA, VIRGINIA 22963

Tristana P. Treadway, Clerk
Sandra A. Parrish, Chief Deputy Clerk

Telephone (434) 591-1970
Facsimile (434) 591-1971

Nancy G. Pace, Deputy Clerk
Cathy A. Allen, Deputy Clerk
Trista L. Robertson, Deputy Clerk
Vincent M. Rizza, Deputy Clerk
Angela F. Lowe, Deputy Clerk
Anayanci L. Frazier, Deputy Clerk

FAX TRANSMISSION

TO: Elizabeth Vaughn, Esq. (703) 443-9362
Hannon Wright, Esq. (540) 301-0021
Samantha Freed, Esq. (434) 979-1221
Kathryn L. Wyer, Esq. (202) 616-8470

FROM: Tristana K. Treadway, Clerk

Counsel:

Attached you will please find the Order Setting Forth Requirements to Secure United States Government Information entered by the Judge on this date. I trust that you will forward to all necessary attorneys and parties.

Thank you.

Tristana P. Treadway, Clerk

VIRGINIA:

IN THE CIRCUIT COURT OF FLUVANNA COUNTY

AMINULLAH AMIN, and FAWZIA AMIN, Petitioners,	**Case No: CL22000186-00**
vs.	**SUBMITTED UNDER SEAL**
JOSHUA & STEPHANIE MAST, Respondents.	

ORDER SETTING FORTH REQUIREMENTS TO SECURE UNITED STATES GOVERNMENT INFORMATION

Pursuant to 28 U.S.C. § 517, the United States has notified the Court that it has identified United States Government information in certain pleadings and documents in this case that must be secured and has requested that the Court take certain actions to secure this information.

UPON CONSIDERATION WHEREOF, the Court hereby ORDERS that the parties, their counsel, the guardian ad litem, and any other individual to whom this information, in whole or in part, has been transmitted (collectively, "Affected Persons") take the following actions:

Each Affected Person shall not further disseminate in any manner and, within five (5) days of this Order, shall permanently delete or destroy any full or partial copy, in whatever form, whether electronic or hardcopy, and in any location, including phone, e-mail or other online accounts, as well as archives or backup files, of the following documents, to the extent they exist within the Affected Person's possession, custody, or control:

1. Respondents' Answer to Complaint, and attachments thereto (filed May 19, 2022)
2. Respondents' Motion for Protective Order, and attachments thereto (filed May 17, 2022)

3. Petitioners' Response to Motion for Protective Order (filed May 20, 2022)

4. E-mail chain containing communications between Joshua Mast and one or more other U.S. servicemembers during the period January 3-5, 2022, with the subject line "Force Protection Incident"

No later than five (5) days of this Order, each Affected Person shall certify to the Court that any full or partial copies of the documents listed above in their possession, custody, or control have been permanently deleted or destroyed as described above and that they have not further disseminated these documents.

Within 5 days of this Order, any document identified above that was filed in this case may be replaced with a substitute filing. Any substitute filing shall omit the images of United States Government information previously attached to Respondents' Answer and Motion for Protective Order, any reference thereto, and any assertion based thereon. Any such substitute filing shall be provided to counsel for the United States by e-mail, at the same time the filing is served on other parties in the case.

REM, but does not need to be,

ENTERED THIS 21st DAY OF October, 2022

JUDGE

EXHIBIT 3

VIRGINIA: IN THE CIRCUIT COURT FOR FLUVANNA COUNTY

AMINULLAH AMIN, and FAWZIA AMIN, Petitioners,	**Case No: CL22000186-00**
vs.	**SUBMITTED UNDER SEAL**
JOSHUA & STEPHANIE MAST, Respondents.	

SUPPLEMENTAL ORDER REGARDING UNITED STATES GOVERNMENT INFORMATION

Pursuant to 28 U.S.C. § 517, the United States has notified the Court that it has identified United States Government information in certain pleadings and documents in this case that must be secured and has requested that the Court take certain actions to secure this information. On October 21, 2022, the Court issued an Order Setting Forth Requirements To Secure United States Government Information ("Order of October 21, 2022"). Since that time, additional documents have been identified that must be secured. The Court also seeks to address the possibility that additional documents may be identified in the future. Accordingly, the Court further orders that:

1. The requirements set forth in the Order of October 21, 2022, shall likewise apply to
    a. Petitioners' Motion in Limine to Exclude Official and Classified Information Absent Express Written Authorization (filed May 19, 2022);
    b. the pages included in an electronic file named "(DOD) TSC.pdf" that was produced by Respondents to Petitioners on May 3, 2022; and
    c. pages bates-stamped as AMIN-0006142, AMIN-0006143, and AMIN-0006144, consisting of an email dated April 14, 2022 and its attachment, produced by Petitioners to Respondents on October 12, 2022.

No later than five (5) business days after entry of this Order, each Affected Person as defined in the Court's Order of October 21, 2022, shall certify to the Court that any full or partial copies of these documents in their possession, custody, or control have been permanently deleted or destroyed as described in the Court's Order of October 21, 2022, and that they have not further disseminated these documents.

2. In the event that the United States identifies additional documents that must be secured, beyond those identified to date, counsel for the United States shall notify the Court and counsel for the parties in this case by e-mail, identifying the documents at issue. Within ten (10) calendar days of receiving such notification, the Affected Persons identified in the Court's Order of October 21, 2022, shall certify to the Court that any full or partial copies of those documents in their possession, custody, or control have been permanently deleted or destroyed, and that they have not further disseminated those documents. Counsel for the United States shall contemporaneously be provided with a copy of such certification by e-mail. If any party or affected person shall have a question, objection, or request for clarification, they shall submit such to the Court within five (5) calendar days of receiving such notice. In such case, the matter will be expedited.

3. To the extent any party wishes to replace a filed document that has been subject to the Court's Order of October 21, 2022, or this Supplemental Order, with a substitute filing, they are granted leave to do so, and the substitute filing shall not consist of a redacted version of the original filing. Any redacted versions of such filings henceforth shall not be accepted by the Clerk of Court and any such redacted versions that have heretofore been submitted shall be removed and deleted from the digital case file and any hard copy originals accepted and filed by the Court shall be kept in a separate secure location, not

accessible to the public, pending further discussions and arrangements by the Clerk of Court with the IT security personnel with the Department of Justice and the Supreme Court of Virginia Office of the Executive Secretary.

ENTERED THIS 28th DAY OF November, 2022

JUDGE